Digital Connection

Don Rotolo, N2IRZ

Computer Security

This document ©2004 by Don Rotolo N2IRZ under CC BY-NC 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc/4.0/.
This document was donated to the Digital Library of Amateur Radio & Communications (DLARC) for public access. It differs slightly from what appeared in *CQ Amateur Radio Magazine*.

Originally in CQ Magazine, February 2004

Just because you're paranoid doesn't mean they're not out to get you. There are some very intelligent folks out there who make their money illegally, by stealing what is yours. In the digital world in which we find ourselves, stealing with a computer is much cleaner than using a gun, and it's harder to get caught, too. Since most hams have a computer and use the Internet, an introduction to the darker side of digital, and some ways to shield yourself against it, seems like a good topic to consider this month.

Computer-based crime is rising, but the amazing thing is that such a large percentage of computer users do absolutely nothing to protect themselves. All anyone has to do is take some simple precautions, and the criminals will probably look elsewhere, kind of like locking your car and taking your keys to prevent your car from getting stolen. Not until most cars are locked will a thief bother to break the glass - it's much easier (and safer) to just move on to an unlocked car. Or computer.

The plain and simple fact is, you need anti-virus software.

Computer security has many aspects. We should worry about people getting into our computer while we're online and hijacking it, as well as people guessing our passwords, or sending nasty software to damage our data. We should also worry about simple mechanical or electrical failure, and ordinary theft of our hardware. Let's look at each of these issues, in turn, and how we can help guard against the problems they may cause.

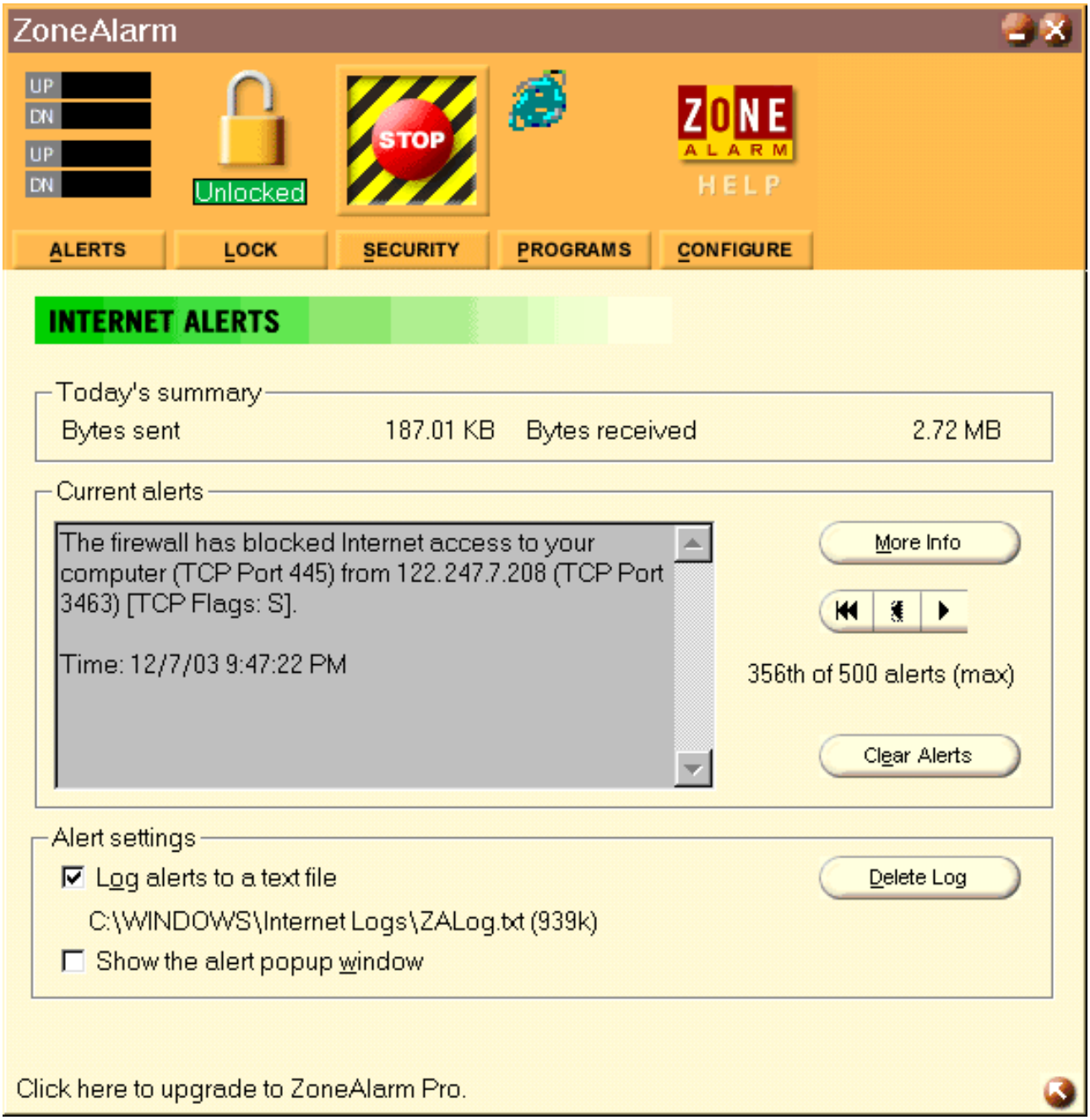
Unauthorized Access, Part 1

Did you know that, unless you have taken specific precautions against it, people can access your computer any time you are online? Here's a test: Go to <http://www.grc.com>, look for "ShieldsUP!" and allow them to test your security for 'common ports'. Unless you have a firewall, you'll be shocked at the results. (Feel free to run the other tests as well). Anyone with some simple software and malicious intent can attack, take control and even damage your computer.

The weak point is your Ports. Various legitimate internet services use specific software hooks or "ports" to access your computer, sort of like virtual COM ports. When connected to the Internet, certain types of Internet applications use certain ports for their work. For example, telnet uses port 23, and http uses port 80. The problem is that there are many ports defined, and if you haven't specifically closed a port, it is open, and it allows access to your computer. A malicious person can use that access for evil, such as destroying your computer, introducing a virus, or using your computer to do evil things to some other computer. This last item is a common tactic in Denial-of-Service attacks against a web site, where some unsuspecting site is so inundated with bogus web hits it cannot serve legitimate users.

The solution is simple and inexpensive: A firewall. Just like a real firewall, which divides a larger building or structure into smaller areas for fire protection, a computer firewall divides a computer network into sections for protection against damage from most 'bad things'. A firewall can be a software program or a piece of hardware that watches all of the communications to and from your computer, allowing only the activity you feel is safe. Note that a pop-up blocker is NOT a firewall.

An older version of Zone Alarm at work. This is a fine example of a software firewall, which prevents any program that you don't specifically enable from sending data to or from your computer. Anyone who uses the Internet needs a firewall. Note that over 500 potential intrusions were blocked, during a single three hour dial-up Internet session. You can download Zone Alarm basic for free - see the text.



Software firewalls are perfectly fine for single computers and small networks. For larger networks, a hardware firewall might offer better speed and performance, since they are optimized for a single purpose. You can download one of the best software firewalls in the business for free from http://www.zonelabs .com, or you can buy the Norton or McAfee firewall software, as well as others.

While broadband users are especially vulnerable, since their Internet connection is active even if it's not being used, having a dial-up connection is no reason for confidence. Without this very basic level of protection, anyone connected to any network is leaving their computer open to attack.

OK, so here is the first task on your To Do list: Obtain and install a firewall for every computer which can connect to the Internet. Most home users would install a software firewall for one to three computers, and perhaps get a hardware firewall for larger installations. Either option is sufficient.

Unauthorized Access, Part 2

If you're alive enough to read this, you surely have at least one password you need to remember. Most of us have literally dozens of password-protected accounts, and if you're like most humans, you use the same password for almost all of them. That's a problem that you must fix right away.

You probably also use a fairly simple password, like "tiger". Or (horrors!) you use a form of your name, birthdate, wedding date, user ID, address, or some other easily-guessed word. If so, STOP IT IMMEDIATELY! You're setting yourself up for a massive security breach, which will definitely take the better part of a few years to clear up. Imagine if someone, just for one night, had complete access to all your accounts? Ever set a password on a web site to get something (for free!)? You may have just given away the keys to your kingdom.

What you need to do is set up a "strong" password system for yourself. By strong, I mean not easily guessed or learned, and by system I mean a way of setting a different password for each and every account you have, but without having to remember dozens of different passwords.

A strong password is at least 6 characters long (I recommend 8 to 12), does not contain all or part of the users account name, and contains at least three of the four following categories of characters: Uppercase characters, lowercase characters, digits 0 through 9, and symbols found on the keyboard (such as !, @, #). For example, "strong" is not a strong password, but "sTr0ng" is.

Come up with a memorable but somewhat random word of about 6 to 8 characters, and make subtle changes to it so that it becomes strong. This will become one of your "core" passwords - you should use different ones for work and home. For example, the word "savings' could be strengthened to "$a1VngS" - nobody would ever guess that, especially how I misspelled it like that.

Even with a strong password like that, using it everywhere defeats the whole purpose. Of course, if you had to remember a different strong password for every single account, you might resort to writing your passwords down - one of the biggest breaches of security you can commit. (If you DO have them written down, don't. OK, maybe one copy for the safe-deposit box, but that's it!). Writing them down won't do, so instead develop a system for each account, using the strong core, but making modifications which only you would know.

Here is an example of a password system you could use. I urge you to come up with a variation on this theme, and make that YOUR system. In this way, all of your passwords will be strong and it will be very unlikely that someone will be able to gain access to any of your accounts in this way. Even if they do get one password, the others will still be secure.

Start with a secure core password, like $a1VngS. Take the first two letters of the site name - like "eb" for eBay.com - and add those to the beginning of the strong core. Then, count the number of characters in the site name - four for "eBay" - and add that to the end of the strong core, resulting in "eb$a1VngS4" for your eBay account, and "pa$a1VngS6" for your PayPal account.

You can see how each account's password will be different and difficult to guess, but easily memorized if you know the system and the core. Please feel free to use the system described, but I strongly recommend making at least some minor changes, such as reversing the letters, or moving the number, or something like that. So, that's the second item on your to-do list: Create and use a strong password system wherever possible.

Oh, one last point related to passwords: If you ever leave your computer unattended, such as when you go to lunch at work, either lock your computer (Ctl-Alt-Del and press Enetr for Win XP and 2000) or at least set your screen saver to require a password. That will help minimize the risk of someone getting onto your computer and, say, sending a letter of resignation from your mail account.

Lightning protection is a given, but thunder protection? These ear plug and their unique carrying case were being handed out by the PolyPhaser folks at Dayton. I use all PolyPhaser equipment for the antennas at my station,

after their book "The Grounds of Lightning Protection" opened my eyes. Good reading, and it shows how any station can be protected against any lightning stroke.

Virus Protection

If you don't know about the threat from computer viruses, you shouldn't be allowed to use a computer. Linux and Mac users might feel more secure, but they also need to understand that a virus can be written for any operating system - Windows just happens to be a big target.

If you do not have anti-virus software on your computer - software that is consistently up-to-date every week, set to screen everything coming in, and that is used regularly and frequently, you do not have any virus protection at all. You might as well save yourself the trouble and format your hard drive - at least there won't be any hardware damage or stolen information.

Yes, that's a strong statement, but not excessively so. The plain and simple fact is, you need anti-virus software. The range of viruses, and the myriad ways they can do harm, demand at least some preventative actions. Looking at the sale flyers from Best Buy, CompUSA, Staples and Office Max, I see that both McAfee Anti-virus 8 and Norton Anti-virus 2004 are on sale for less than $20, and there's even a rebate if you're upgrading. You're even entitled to at least a year's worth of free updates to the virus definition files. For $20, consider it health insurance for your computer, and let it go. If the money is an issue, you can get free virus scans at the McAfee and Symantic (Norton) web sites.

Since many more people have, maintain and use Anti-virus software than firewalls, this issue is only number three on our hit parade. Nonetheless, those who have no virus protection, or don't keep their updated, are just sitting ducks, driving with their eyes closed - something bad will happen, sooner than later, and a few bucks for protection will then seem like a cheap price to pay. The need for Anti-virus software applies even if you don't have Internet access - that floppy or CD you borrowed is just as effective for infecting your computer. So, the third item on your To Do list is: Get, maintain and use Anti-virus software. The key word is maintain: an ounce of prevention is worth a pound of cure.

Plain old troubles

After looking at some of the electronic pitfalls awaiting us, these next few will seem like old friends - or enemies, really. But, we tend to be more comfortable around familiar foes than unfamiliar ones. Nonetheless, these old foes are just as troublesome as ever, lest we forget.

The first of these is plain old theft. While you're on break at a conference, someone lifts your laptop. With your company's confidential new product plan. Oops! Laptops, and even to a lesser degree, desktop computers are like pets or children: You need to keep your eyes on them, because it only takes a second for them to go missing.

To prevent hardware from walking out the door too easily, use brute force. One of those cheap laptop locking cables is a good idea. Sure, a determined thief can defeat the lock in under a minute (I've seen it), maybe it'll make the thief pick up someone else's laptop instead. Good enough. Same idea works with desktop systems, too. Like the old joke goes, you don't have to outrun the bear, just outrun your buddy.

The second is externally induced mechanical or electrical failure. The simple version is to make sure the expensive hardware is protected against water, falling, things falling on it, and the like. The subtle version is to protect against power surges and lightning strikes. After all, protecting a PC is a lot easier than protecting a transceiver.

Get a mid-priced surge protector for the PC's power input and any communications lines, like the phone or network wiring. The $5 surge protectors are worse than worthless, since you're fooled into thinking they are effective. I've seen surge protectors in the $25 range that are generally sufficient. On my own equipment, I use an ISO-BAR (with RF filtering) that cost $85 fourteen years ago, along with a whole-house surge suppressor installed in the main breaker panel ($65 plus installation, definitely not a DIY job), and an inexpensive Belkin Surge-Master switch box. I don't think it's overkill.

The last major foe is plain old Hard Disk failure. It happens more often than you think, and you're a candidate as long as you have a hard disk. The solution is a simple backup, done regularly. Whether you use floppies, a tape drive, or recordable CDs or DVDs, you need to store copies of your most important data somewhere that isn't on your hard drive. These days, with the price of hard disks so low (120 GB costs less than $80, retail), it might even make sense for you to buy a new hard disk, copy everything onto it, and unplug it again so it can't get damaged.

Although a complete backup and restoration set for your entire computer is the ideal solution, it may be impractical on a regular basis. Also, consider that not everything needs to be backed up. Things like your operating system and software packages, which can be reinstalled from their original disks, don't really need to be backed up. In the event of a catastrophe, all you need backups of are the files which you created or changed. For Windows users, the contents of the "My Documents" folder would be a good start. Look for any other items that can't be downloaded or otherwise replaced, and back those up, too.

There are many utilities that can be used for a regular backup program. Windows comes with one, my CD burner came with one, and there are a few freeware and shareware versions available for download. You can also buy a backup utility - they are very reasonably priced - and (trust me) if you ever have to do a restore, you will be so happy you had a backup copy made.

Which brings up to the fourth item on your To Do list: Make regular data backups for when your surge protector blows up. Or your laptop is stolen.

There you have it: computer security in a nutshell.

With only four items on your list, you should have no trouble completing these by the time April's issue of CQ shows up. If you take the time to do them you'll have a solid and stable computing system, safe from evildoers, which will bring you happiness and pleasure for years to come. At least, it will be less painful when something does go wrong.

Good luck & 73.
-Don, N2IRZ